UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

Black Samsung smartphone with IMEI 350603974641650 and telephone number 2678942794; black iPhone with a black Otter Box case; green iPhone with a black Otter Box case; black UMX smartphone; purple Motorola smartphone with IMEI 357902518722406 with a black case; and white iPad with IMEI 012923000709070

Case No. 23-mj-523

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Distribution of a controlled substance
21 U.S.C. § 846	Conspiracy to distribute a controlled substance

The application is based on these facts:

See attached Affidavit, incorporated herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Scott C. Smyth

Applicant's signature

SA Scott C. Smyth, DEA

Printed name and title

Sworn to before me and signed in my presence.

Date: 03/13/23

/s/ Richard A. Lloret

Judge's signature

City and state: Philadelphia PA

The Honorable Richard A. Lloret, U.S.M.J.

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Black Samsung smartphone with IMEI 350603974641650 and telephone number 2678942794; black iPhone with a black Otter Box case; green iPhone with a black Otter Box case; black UMX smartphone; purple Motorola smartphone with IMEI 357902518722406 with a black case; and white iPad with IMEI 012923000709070

Case No. 23-mj-523

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before March 27, 2023 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the duty magistrate.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 3/13/23 at 12:42 PM

/s/ Richard A. Lloret
Judge's signature

City and state: Philadelphia, PA

Richard A. Lloret, U.S.M.J.
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 23-mj-523	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

AFFIDAVIT

I, Scott C. Smyth, a Special Agent with the Drug Enforcement Administration (DEA), being duly sworn, deposes and states:

Introduction

1. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

2. Your affiant is a Special Agent with the Drug Enforcement Administration (DEA) in Philadelphia, Pennsylvania, assigned to the Philadelphia Division Enforcement Group 21, which investigates narcotics trafficking.

3. Your affiant has been employed as a DEA Special Agent since July 2020. Your affiant has received specialized training from the DEA Academy at Quantico, Virginia, in the investigation and identification of narcotics traffickers, and has participated in numerous investigations, which have led to the arrests of numerous narcotics traffickers. Your affiant has conducted physical and electronic surveillance, debriefed confidential sources, interviewed witnesses, worked with experienced federal, state, and local narcotic agents and officers, executed search warrants, and analyzed telephone toll records. Prior to joining the DEA, I worked as an Anti-Money Laundering Specialist at Digital Federal Credit Union. During my time in this role, I participated in numerous investigations into money laundering and other violations of the Bank Secrecy Act.

4. From training and experience during my time with the DEA, your affiant has become familiar with the methods and techniques associated with the distribution of narcotics, the laundering of drug proceeds, and the organization of drug conspiracies and drug trafficking

organizations. Your affiant is familiar with the clandestine manner in which cocaine, crack, heroin, marijuana, methamphetamine, and other controlled substances are manufactured, sold, distributed, and used. Your affiant is also familiar with prices, slang terminology, codes, and mechanisms used in association with the distribution and use of illicit narcotics.

PURPOSE OF AFFIDAVIT

5. Your affiant submits this affidavit in support of an application for a search warrant for the following devices: One black Samsung smartphone with IMEI 350603974641650 and telephone number 2678942794 (SUBJECT DEVICE 1); black iPhone with a black Otter Box case (SUBJECT DEVICE 2); iPhone with a black Otter Box case (SUBJECT DEVICE 3); black UMX smartphone, (SUBJECT DEVICE 4); Motorola smartphone with IMEI 357902518722406 with a black case (SUBJECT DEVICE 5); and white iPad with IMEI 012923000709070 (SUBJECT DEVICE 6). This application seeks authority to search the SUBJECT DEVICES (six total) and seize evidence of crimes against the United States, specifically violations of Title 21, United States Code, Section 841(a)(1) and 846 as described in Attachment B.

6. As set forth below, there is probable cause to believe that the SUBJECT DEVICES have been used in the commission of crimes, including violations of Title 21, United States Code, Sections 841(a)(1) and 846 (distribution of controlled substances, the use of communication facilities to commit a controlled substance offense and conspiracy to commit controlled substance offenses). Because this affidavit is submitted for the limited purpose stated above, it does not include every fact known to me about the investigation, but only those facts establishing probable cause to search the contents of the SUBJECT DEVICES.

FACTS ESTABLISHING PROBABLE CAUSE

7. During the month of October 2022, a Pennsylvania State Police confidential source[1] (hereinafter referred to as "CS") provided information to Pennsylvania State Police Trooper Ryan Tierney and SA Nicholas DiFrancesco that he/she was aware of an individual who is from the Philadelphia area of Pennsylvania who is involved in the distribution of large quantities of methamphetamine and other narcotics. The CS was familiar with the individual as he/she knows the individual from being previously involved in methamphetamine trafficking activities. The CS described the individual as a black male known to him/her as "Marc". The CS stated that "Marc" was involved in the distribution of large quantities of methamphetamine and other narcotics, throughout the City and County of Philadelphia and surrounding counties in Pennsylvania. The CS stated that as recent as the late weeks of October 2022, he/she had spoken with "Marc" in regard to purchasing methamphetamine. The CS advised that "Marc" sells multiple pound quantities of methamphetamine as he/she has purchased methamphetamine from "Marc" in the past. The CS advised that "Marc" utilizes telephone number 267-894-2794, known to be associated with SUBJECT DEVICE 1, to coordinate the sale of methamphetamine.

8. Investigators subsequently identified the user of SUBJECT DEVICE 1 as defendant, Jamar DAVIS.

9. On December 1, 2022, physical surveillance was being conducted on DAVIS while he was utilizing his silver Buick Lacrosse. During the course of surveillance, investigators observed the Buick parked directly in front of Sweeny's bar, located at 13639 Philmont Ave., Philadelphia, PA. A member of the Pennsylvania State Police acting in an undercover capacity

[1] The CS was arrested part of a Pennsylvania State Police drug investigation during May of 2022. The CS is not currently paid. Investigators have corroborated information provided by the CS. The CS is currently working with law enforcement for consideration at sentencing.

(hereinafter referred to as "UC") entered the bar and sat down. At this time, the UC observed DAVIS sitting alone at the bar, and positively identified the individual as Jamar DAVIS. While at the bar, the UC and DAVIS engaged in conversation. During this conversation, DAVIS stated that he was owner/operator of a trucking business. DAVIS showed the UC a picture of a tractor trailer with a red tractor and a white trailer. DAVIS said that he has a son who is six (6) years old, and that everything is in his name. DAVIS then initiated a drug related conversation with this UC during which he related to the UC that he used to be "that guy" and could get the UC whatever he/she needed. The UC advised investigators that he/she believed that DAVIS was referring to drugs. DAVIS then explained what he referred to as a hypothetical situation to the UC. DAVIS explained that if he (DAVIS) provided the UC with ten (10) pounds of methamphetamine at a cost of $1,500.00 per pound, DAVIS would "front" the UC an additional ten (10) pounds, for a total of 20 pounds.

10. From my training and experience, I know that "fronting" is a slang term used by drug traffickers when a quantity of controlled substances is provided to someone, with the understanding that after the recipient sells the narcotics and receives money, that recipient will return to the supplier with payment for the drugs previously supplied.

11. DAVIS stated that he would get the methamphetamine to the Philadelphia area, and that the UC would not have to worry about that portion of the operation. DAVIS then outlined what money would be owed to DAVIS for the quantity of methamphetamine that he "fronted" to the UC. DAVIS also asked the UC what he/she would do if arrested during the course of these activities. DAVIS provided the UC with telephone number (267)-894-2794 (SUBJECT DEVICE 1) for the purpose of contacting him in the future and identified himself as "Marc" to the UC.

DAVIS also indicated to the UC that he lives "around the corner" from this location (Sweeny's bar), which is consistent with the observations made by investigators during this investigation.

12. In December 2022, the UC purchased approximately one pound of methamphetamine from Jamar DAVIS. The UC and DAVIS coordinated this meeting and drug transaction through SUBJECT DEVICE 1. DEA Laboratory results revealed that the acquired drug exhibit was approximately 444.6 grams of 98% pure methamphetamine.

13. In January 2023, the UC purchased approximately six pounds of methamphetamine from Jamar DAVIS. The UC and DAVIS coordinated this meeting and drug transaction through SUBJECT DEVICE 1. DEA Laboratory results revealed that the acquired drug exhibit was approximately 2,658 grams of 97% pure methamphetamine.

14. On January 27, 2023, the Honorable Richard A. Lloret, United States Magistrate Judge for the Eastern District of Pennsylvania signed order 23-mj-184-1, authorizing the search of 152 Brookshire Drive, Philadelphia, PA, among other locations.

15. Electronic surveillance of the device associated with telephone number 2678942794 (SUBJECT DEVICE 1) and physical surveillance of 152 Brookshire Drive, Philadelphia, PA, supported that DAVIS was present at this address frequently, including during late night and early morning hours. Based upon these observations, Investigators concluded that 152 Brookshire Drive, Philadelphia, PA, was DAVIS' primary residence.

16. On January 28, 2023, agents from DEA Philadelphia and members of the Pennsylvania State Police (together identified as "Investigators") executed the above-mentioned federal search warrants.

17. Among the evidence recovered at 152 Brookshire Dr. Philadelphia, PA, Investigators located and seized approximately twelve (12) pounds of a mixture and substance

containing methamphetamine and two privately made firearms, extended magazines, a money counter, and the SUBJECT DEVICES. The SUBJECT DEVICES were all located in DAVIS' bedroom and DAVIS advised investigators that the SUBJECT DEVICES were all his. DEA Laboratory results revealed that the acquired drug exhibit was approximately 5,370 grams of 98% purity methamphetamine.

18. Your affiant is also aware through training and experience that drug traffickers often use multiple cell phones to create separation between their communications with customers and their communications with family or members of the organization and as a way to thwart detection by law enforcement. Therefore, your affiant believes that the SUBJECT DEVICES will contain evidence of the crimes committed outlined above.

REQUEST TO SEARCH CELLULAR TELEPHONES

19. Based on training and experience, your affiant knows that individuals involved in drug trafficking often maintain more than one phone or more than one SIM card device, in order to have multiple avenues to facilitate drug trafficking activities, and in an attempt to avoid detection by law enforcement. Your affiant is aware that individuals involved in drug trafficking often utilize pre-paid cellular telephones which do not maintain specific subscriber information, and/or use phones subscribed to in the name of third person, to mask their direct linkage to telephones utilized in furtherance of drug trafficking activities. Further, those involved in drug trafficking often change SIM cards in order to make it difficult for law enforcement to determine their records. Based on my training and experience, your affiant knows that individuals involved in drug trafficking also frequently switch telephone numbers and/or phones. Despite the constant switching of active telephone numbers, drug traffickers often keep old phones.

20. Based on training and experience, your affiant knows drug traffickers commonly utilize their cellular telephones to communicate with co-conspirators to facilitate, plan, and execute their drug transactions. For example, your affiant knows that drug traffickers often store contacts lists, address books, calendars, photographs, videos, and audio files, text messages, call logs, and voice mails in their electronic devices, such as cellular telephones, to be used in furtherance of their drug trafficking activities.

21. Your affiant knows that those involved in drug trafficking communicate with associates using cellular telephones to make telephone calls. If they are unable to reach the party called, they frequently leave voice mail messages. Your affiant is aware that Apple-based and Android-based phones download voice mail messages and store them on the phone itself so that there is no need for the user to call in to a number at a remote location and listen to the message. In addition, your affiant knows that those involved in drug trafficking communicate with associates using cellular telephones and tablets to send e-mails and text messages and communicate via social media networking sites. By analyzing call and text communications, your affiant may be able to determine the identity of co-conspirators and associated telephone numbers, as well as if there were communications between associates during the commission of the crimes.

22. Furthermore, cellular telephones also contain address books with names, addresses, photographs, and phone numbers of a person's regular contacts. Your affiant is aware that drug traffickers frequently list drug associates in directories, often by nickname, to avoid detection by others. Such directories as the ones likely contained in the seized cellular telephones, are one of the few ways to verify the numbers (*i.e.*, telephones, pagers, etc.) being used by specific traffickers.

23. In addition, your affiant knows that those involved with drug trafficking often take photographs or make videos of themselves and their co-conspirators and retain them on their electronic devices such as cellular telephones. This evidence would show associations between accomplices, *i.e.* photographs of accomplices and/or individuals common to co-conspirators. Your affiant is also aware that drug traffickers often take photographs or make videos of drugs and drug proceeds with their cellular telephones and tablets. Based on my training and experience, those who commit these crimes often store these items on their phones in order to show to associates, and/or to upload to social media.

24. Furthermore, based on training and experience, your affiant knows drug traffickers often use a cellular phone's Internet browser for web browsing activity related to their drug trafficking activities. Specifically, drug traffickers may use an Internet search engine to explore where banks or mail delivery services are located, or may use the Internet to make reservations for drug-related travel. In addition, your affiant knows that drug traffickers also use their cellular telephone's Internet browser to update their social networking sites in order to communicate with co-conspirators, display drugs and drug proceeds, or to post photographs of locations where they have traveled in furtherance of their drug trafficking activities.

25. In addition, drug traffickers sometimes use cellular telephones as navigation devices, obtaining maps and directions to various locations in furtherance of their drug trafficking activities. These electronic devices may also contain GPS navigation capabilities and stored information that could identify where these devices were located.

26. Furthermore, based on my training and experience, forensic evidence recovered from the review of a cellular telephone can also assist in establishing the identity of the user of the device, how the device was used, the purpose of its use, and when it was used. In particular,

your affiant is aware that cellular telephones are all identifiable by unique numbers on each phone, including: serial numbers, international mobile equipment identification numbers (IMEI) and/or electronic serial numbers (ESN). The search of each phone helps determine the telephone number assigned to each device, thus facilitating the identification of the phone as being used by members of the conspiracy. In addition, your affiant is aware forensic tools may uncover information/data users have deleted which may still be able to be recovered from the device.

ELECTRONIC DEVICES

27. As described above and in Attachments A and B, this application seeks permission to search and seize things that the above item might contain, in whatever form they are stored. As used herein, the term "electronic device" includes any electronic system or device capable of storing or processing data in digital form, in this case referring specifically to wireless or cellular telephones.

28. Based on training and experience, as well as information relayed to me by others involved in the forensic examination of electronic/digital devices, your affiant knows data in digital form can be stored on a variety of digital devices. In particular, your affiant knows electronic devices, including cellular telephones used by drug traffickers and digital/computing devices, are likely to be repositories of evidence of crimes. Your affiant knows an electronic device such as a cellular telephone may contain data that is evidence of how the electronic device was used, data that was sent and received, and other records that may indicate the nature of the offense.

29. Furthermore, your affiant knows that electronic devices, such as cellular telephones and computers, can store information for long periods of time. Examples of such information include text and multimedia message conversations, call history, voice mail

messages, e-mails, photographs, and other data stored on the device. Similarly, your affiant knows, from training and experience, when cellular telephones or electronic devices are used to access the internet, a browser history is also frequently stored for some period of time on the electronic device. This information can sometimes be recovered with forensic tools.

30. Based on my experience and training, as well as the experience and training of other agents, your affiant knows that even when a user deletes information from a device, it can sometimes be recovered with forensic tools.

31. Based on training and experience, as well as information related by agents and others involved in the forensic examination of electronic devices, your affiant knows that searching electronic devices can be a highly technical process that requires specific expertise and specialized equipment. There are many types of electronic devices and software programs in use today which require specialized equipment to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of electronic devices, operating systems, or software applications being searched.

32. Furthermore, your affiant is aware that electronic data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching electronic devices can require the use of precise, scientific procedures that are designed to maintain the integrity of electronic data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on electronic devices.

33. Also, your affiant knows from my training and experience that the volume of data stored on many electronic devices will typically be so large it will require a search of the device in a law enforcement laboratory or similar facility. A single megabyte of storage space is the

equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

34. Your affiant is also aware that electronic files or remnants of such files can be recovered months or years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. Normally, when a person deletes a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and

computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time

35. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), electronic devices can contain other forms of electronic evidence as well. In particular, records of how an electronic device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the electronic devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregated from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the electronic device was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

36. Further, evidence of how an electronic device has been used, what it has been used for, and who has used it, may be the absence of particular data on an electronic device. For example, to rebut a claim that the owner of an electronic device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the electronic device remotely is not present on the electronic device. Evidence of the absence of particular data on an electronic device is not segregated from the electronic device. Analysis of the electronic device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

37. Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time consuming manual search through unrelated materials that may be co-mingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the DEA intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

38. Your affiant therefore believes and asserts that a search of the electronic files and memory of the SUBJECT DEVICES will yield evidence of violations of the federal laws, including, but not limited to, disclosing the identities of persons involved in the commission of these offenses, as well as the existence and scope of the conspiracy. Evidence of calls made by, to, and among the members of this conspiracy, in the course of the events related in this affidavit, are also expected to be disclosed by the requested search.

39. Therefore, based on the information, facts and circumstances stated above, your affiant believes the SUBJECT DEVICES, seized by law enforcement, will provide investigators with additional information related to the ongoing investigation of DAVIS and other unknowns who are involved in narcotics trafficking. Accordingly, I respectfully request that the Court issue a warrant to search the SUBJECT DEVICES.

SUMMARY AND CONCLUSION

40. Based upon the foregoing facts, your affiant submits there is probable cause the fruits and/or evidence of crimes, specifically, violations of Title 21, United States Code, Sections 841(a)(1) and 846, will be found in the information stored in the SUBJECT DEVICES identified in Attachments A. These phones have remained in the secure custody of DEA in Philadelphia, Pennsylvania, since the arrest of DAVIS on January 28, 2023.

41. Your affiant declares under penalty of perjury that the foregoing is true and correct to the best of her knowledge and belief.

/s/ Scott C. Smyth
Scott C. Smyth
Special Agent
Drug Enforcement Administration

Subscribed to and sworn before me this
__13___ day of March, 2023.

/s/ Richard A. Lloret
HONORABLE RICHARD A. LLORET
United States Magistrate Judge

ATTACHMENT A
(Property to be Searched)

1. Black Samsung smartphone with IMEI 350603974641650 and telephone number 267-894-2794 (SUBJECT DEVICE 1)
2. Black iPhone with a black Otter Box case (SUBJECT DEVICE 2)
3. Green iPhone with a black Otter Box case (SUBJECT DEVICE 3)
4. Black UMX smartphone, (SUBJECT DEVICE 4)
5. Purple Motorola smartphone with IMEI 357902518722406 with a black case (SUBJECT DEVICE 5)
6. White iPad with IMEI 012923000709070 (SUBJECT DEVICE 6)

ATTACHMENT B
(Property to be Seized)

1. All records contained in the SUBJECT DEVICES that relate to violations of the statutes Title 21, United States Code, Sections 841(a)(1) and 846, and involve DAVIS including:
    a. lists of customers and related identifying information;
    b. information concerning the types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
    c. any information related to sources of drugs, including names; addresses, phone numbers, or any other identifying information;
    d. any information related to the methods of trafficking in drugs;
    e. any information recording domestic and international schedule or travel; and
    f. all bank records, checks, credit card bills, account information, and other financial records.
2. Evidence of user attribution showing who used or owned the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including:
    a. Any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.
    b. All data that has been manually programmed into a GPS navigation system, as well as data automatically stored by the GPS navigation system, including any and all electronic data which can be collected, analyzed, created, displayed,

converted, stored, concealed, or transmitted, or similar computer impulses or data.

c. Stored electronic information and communications, including telephone or address directory entries consisting of names, addresses and telephone numbers; logs of telephone numbers dialed, telephone numbers of missed calls, telephone numbers of incoming calls; schedule entries; stored memoranda; stored text messages; stored photographs; store audio; and stored video.